

described in the background portion of the application, particularly at pages 5-8, computations involving the private key make it vulnerable to detection by means of differential power analysis (DPA). In accordance with the present invention, this vulnerability is reduced by masking the private key with the use of a random value having the same length as the private key. This masking procedure is set forth in the five steps of claim 1.

The *Miyazaki* reference does not discuss attacks on secret keys, such as those based upon DPA, and therefore does not disclose a countermeasure for protecting against such types of attacks. Rather, the *Miyazaki* reference is concerned with the ability to share secret information among a number of people, so that if a secret key is lost or destroyed, encrypted data can be decrypted with the use of the shared information. See, in general, the summary of the invention that begins at column 1, line 55 of the *Miyazaki* patent.

As such, the *Miyazaki* reference does not disclose the sequence of steps recited in claim 1 for masking a private key as a countermeasure against PDA attacks. For example, the first two steps of claim 1 recite selecting a random value r with the same size as the private key d , and calculating an integer $d' = d + r$. The Office Action refers to the *Miyazaki* patent's teaching of selecting a random number k that has a bit length equal to that of the secret key, at column 3, lines 43-46. However, the reference does not disclose that this random number is summed with the private key to generate a masking integer. Rather, at steps 203-206 described in column 3, lines 47-59, the random number k is multiplied with each of four different *public* keys $Q1$ - $Q4$, to generate four (x,y) pairs. See also Figure 2. The *Miyazaki* reference does not disclose, nor otherwise suggest, that the random number k is summed with the private key.

Claim 1 recites the further steps of performing a scalar multiplication operation $d' \cdot P$, to obtain a point Q' on an elliptic curve, and deriving another point Q on the curve by the operation $Q = Q' - S$, where $S = r \cdot P$. In connection with this claimed subject matter, the Office Action refers to the *Miyazaki* patent at column 4, lines 55-58, which discloses that a point P on an elliptic curve is multiplied by the random number k to obtain a value $R(x,y)$. Even if the value R can be considered to correspond to the point S in claim 1, there is no disclosure in the *Miyazaki* patent that this point is used to calculate another point Q on the elliptic curve, such that $Q = d \cdot P$.

As set forth in MPEP 2131, to anticipate a claim, the reference must teach *every* element of the claim. For at least the reasons presented above, it is respectfully submitted that the *Miyazaki* reference does not anticipate any of claims 1, 2 or 13, since it does not teach every element of those claims. For the same reasons, it does not suggest the subject matter of claims 3-12, whether considered by itself or in combination with the *Koblitz* publication.

Claims 1, 2 and 13 were also rejected under 35 U.S.C. §102, on the grounds that they were considered to be unpatentable over the *Kocher et al.* publication, entitled "Differential Power Analysis". Claims 1-13 were rejected under 35 U.S.C. §103, as being unpatentable over the *Koblitz* publication in view of the *Kocher* publication.

The *Kocher* publication is directed to differential power analysis, per se, and describes the basic theory that underlies these types of attacks on the privacy of encryption keys. In Section 6 of the publication, appearing on pages 8 and 9, it generally describes the three categories of techniques for preventing DPA attacks. As noted in the Office Action, these categories include the use of non-linear key update procedures that are based upon


hashing functions, and use counters to minimize the number of samples available to an attacker. The reference does not disclose, however, the specific countermeasure procedure set forth in the claims. The Office Action has not identified where any of the steps recited in claim 1, for example, are taught by the *Kocher* publication. The mere fact that the *Kocher* publication recognizes that countermeasure techniques are available does not inherently suggest the claimed subject matter to a person of ordinary skill in the art. The *Kocher* publication does not teach every element of the rejected claims.

The *Koblitz* publication is apparently being cited for its disclosure relating to doubling-and-add operations. The publication does not, however, disclose those features of the claimed subject matter which are missing from the *Kocher* publication, such as the steps recited in claim 1. Accordingly, it is respectfully submitted that the *Kocher* publication does not suggest the claimed subject matter to a person of ordinary skill in the art, whether considered by itself or in combination with the *Koblitz* publication.

For the foregoing reasons, it is respectfully submitted that the pending claims are patentably distinct from the references of record. Reconsideration and withdrawal of the rejections are respectfully requested.

Respectfully submitted,
BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: November 10, 2004

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620